Installation and Deployment Guide

Websense® Endpoint Solutions, v8.0.x

v8.0.x

©2014, Websense Inc.
All rights reserved.
10900 Stonelake Blvd, 3rd Floor, Austin, TX 78759, USA

Published 2014
Printed in the United States and Ireland

The products and/or methods of use described in this document are covered by U.S. Patent Numbers 5,983,270; 6,606,659; 6,947,985; 7,185,015; 7,194,464 and RE40,187 and other patents pending.

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Websense Inc.

Every effort has been made to ensure the accuracy of this manual. However, Websense Inc., makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Websense Inc., shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Trademarks

Websense and TRITON are registered trademarks of Websense, Inc., in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Mozilla and Firefox are registered trademarks of the Mozilla Foundation in the United States and/or other countries.

This product includes software distributed by the Apache Software Foundation (http://www.apache.org).
Copyright (c) 2000. The Apache Software Foundation. All rights reserved.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Contents

Topic 1 **Introducing Websense Endpoint Solutions 1**

TRITON AP-ENDPOINT Web 2
TRITON AP-ENDPOINT DLP 3
System requirements 3
Hardware requirements 3
Operating system requirements 4
Browser support 5
TRITON AP-ENDPOINT Web 5
TRITON AP-ENDPOINT DLP 5
DLP channel support 6
Email clients 6
Printer drivers 6
Application controls 6
Supported removable media 7
LAN control 7
Destination channels by operating system 7

Topic 2 **Obtaining or Creating the Installation Package 9**

Downloading installation packages from the TRITON Manager 9
On-premises TRITON Manager (hybrid deployments) 10
Cloud TRITON Manager (cloud deployments) 10
Creating installation packages from a package builder 10
TRITON AP-ENDPOINT DLP module 15
TRITON AP-ENDPOINT Web 17
Remote filter 18
Global settings 21

Topic 3 **Deploying endpoint software in Your Enterprise 21**

Before you begin 21
Disabling automatic updates for TRITON AP-ENDPOINT Web 22
Enabling automatic updates 22
Deploying Windows endpoints 23
Manual deployment 23
Testing deployment 25
Deploying Mac endpoints 25
Manual deployment 25
Testing deployment 26
Deploying Linux endpoints (stand-alone DLP only) 26
Configuring and managing endpoints 27

Uninstalling endpoint software. 28
Windows uninstallation. 28
Local uninstallation 28
Remote uninstallation with deployment server 29
Remote uninstallation using distribution systems 29
Mac uninstallation. 30
Linux uninstallation (stand-alone DLP only) 30

Introducing Websense Endpoint Solutions

Applies to:	In this topic
◆ TRITON AP-WEB v8.0.x ◆ TRITON AP-DATA v8.0.x ◆ Web Filter & Security v8.0.x ◆ TRITON AP-ENDPOINT Web v8.0.x ◆ TRITON AP-ENDPOINT DLP v8.0.x	◆ *TRITON AP-ENDPOINT Web* ◆ *TRITON AP-ENDPOINT DLP* ◆ *Hardware requirements* ◆ *Operating system requirements* ◆ *Browser support* ◆ *DLP channel support*

Websense® endpoint solutions provide complete real-time protection against advanced threats and data theft for both network and roaming users. Websense advanced technologies help you discover and protect sensitive data stored on endpoint clients and provide actionable forensic insight into potential attacks.

- Websense offers 2 endpoint web protection options to protect users from web threats:
  - TRITON AP-ENDPOINT Web—requires a TRITON AP-WEB on-premises solution with the Web Hybrid module (Windows only) or TRITON AP-WEB with the Web Cloud module.
  - Remote Filtering Client—requires Web Filter & Security with the Remote Filter module.
- TRITON AP-ENDPOINT DLP protects organizations from data loss and data theft. It also identifies and remediates sensitive data stored on corporate computers, including laptops. Requires TRITON AP-DATA Gateway or Discover.

For TRITON AP-ENDPOINT DLP, Remote Filtering Client, or mixed deployments that combine TRITON AP-ENDPOINT DLP and TRITON AP-ENDPOINT Web, you can use a package builder utility to generate **endpoint client software** that runs on the endpoint clients to block, monitor, and log transactions (like Internet requests or proprietary data sharing) according to the organization's security and acceptable use policies. Administrators can create policies that provide full visibility into inbound and outbound traffic, but that don't restrict use of the client computer.

Websense solutions include endpoint **server components** as well. These are part of your TRITON AP-WEB or TRITON AP-DATA deployments.

See *System requirements*, page 3 for information about the hardware requirements for endpoint client components.

About this guide

This guide describes how to deploy Websense software on endpoint client machines across your enterprise.

- Chapter 1 describes system requirements, browser and operating support, benefits, and other information.
- Chapter 2 describes how to obtain or create installation packages.
- Chapter 3 describes how to globally deploy software and install it on endpoint clients.

Related materials

- *Server installation* - Websense endpoint solutions rely on other Websense products for server-side functions. If you haven't already, you must install these products before beginning.
  - Installing TRITON AP-DATA (for DLP)
  - Installing TRITON AP-WEB (for hybrid web deployment)
  - No installation required (cloud web deployment)
  - Installing Web Filter & Security (for Remote Filtering)
- *Endpoint configuration* - Once the endpoint software is deployed to your client machines, you configure it in the TRITON Manager.
  - Web Security Manager Help
  - Data Security Manager Help
  - Cloud TRITON Manager Help
- *Client software usage* - If the software is not installed in stealth mode, users can interact with the user interface.
  - End User Guide for Websense Endpoint Solutions

TRITON AP-ENDPOINT Web

In TRITON AP-WEB deployments, Websense TRITON AP-ENDPOINT Web can be used to secure client machines whose Internet activity is managed by the hybrid or cloud service. TRITON AP-ENDPOINT Web provides transparent authentication and enforces the use of hybrid or cloud web protection policies.

TRITON AP-ENDPOINT Web routes Internet requests to the hybrid or cloud service so that the appropriate policy can be applied.

- TRITON AP-ENDPOINT Web redirects HTTP and HTTPS traffic to the hybrid or cloud service with an encrypted token that identifies the user, enabling the correct policy to be applied and reporting data to be correctly logged. No password or other security information is included.

- For supported browsers, TRITON AP-ENDPOINT Web manipulates proxy settings in real time. For example, if TRITON AP-ENDPOINT Web detects it is at a hotspot, but the user has not finished registration, it removes its proxy settings until the gateway has successfully opened.

You can enable TRITON AP-ENDPOINT Web for some or all machines managed by the cloud or hybrid service.

In Web Filter & Security deployments, you can add the Remote Filter module to manage Internet requests from machines outside the network. By default, remote filtering software monitors HTTP, HTTPS, and FTP traffic. You cannot install Remote Filter and the hybrid or cloud web endpoint on the same machine.

TRITON AP-ENDPOINT DLP

The Data Loss Prevention (DLP) component of TRITON AP-ENDPOINT is designed for organizations concerned about data loss originated at the endpoint, whether malicious or inadvertent. For example, if you want to prevent employees from taking sensitive data home on their laptops and printing it, posting to the Web, or copy and pasting it, you would benefit from this endpoint solution.

Websense TRITON AP-ENDPOINT DLP is a comprehensive, secure and easy-to-use endpoint data loss prevention (DLP) solution. It monitors real-time traffic and applies customized DLP policies over application and storage interfaces. You can also apply discovery policies to endpoints to determine what sensitive data they hold.

You can monitor user activity inside endpoint applications, such as the cut, copy, paste, print, and print screen operations. You can also monitor endpoint web activities and know when users are copying data to external drives.

System requirements

Hardware requirements

Windows

Windows clients must meet the following minimal hardware requirements.

- Pentium 4 (1.8 GHz or above)
- At least 850 MB free hard disk space (250 MB for installation, 600 MB for operation)
- At least 512 MB RAM on Windows XP
- At least 1GB RAM on Windows Vista, Windows 7, Windows 8, Windows Server 2003, Windows Server 2008, Windows Server 2012

Mac

Mac clients must meet the following minimal requirements.

- At least 1 GB RAM
- At least 500 MB free hard disk space (375 MB for installation, 125 MB for operation)

Linux (stand-alone DLP only)

- At least 1 GB RAM
- 1 GB free hard disk space (not including contained files and temporary buffers; see the Data Security Manager Help for information about contained files and allocating enough disk storage for them)

Operating system requirements

Endpoint clients must be running one of the following operating systems:

Operating System	32-bit	64-bit
Windows 7 with Service Pack 1	✓	✓
Windows 8 Windows 8.1	✓	✓
Windows Vista with Service Pack 1 or higher	✓	✓
Windows XP with Service Pack 3	✓	✓
Windows Server 2003 with Service Pack 2	✓	✓
Windows Server 2008 with Service Pack 2	✓	✓
Windows Server 2008 R2 with Service Pack 1		✓
Windows Server 2012 R2		✓
Mac OS X 10.7, 10.8 Mac OS X 10.9		✓

Red Hat Enterprise Linux/CentOS 5.1 with stock kernel 2.6.18-53* (TRITON AP-ENDPOINT DLP only)	✓	✓

Note: by default, Windows Server 2003 or XP support only 3 agents per client. If your endpoint clients will be running multiple agents—for example the endpoint agent, an antivirus agent, and an antispam agent—you must modify their registry entries.

*The Linux DLP endpoint requires FUSE support to enable USB detection. If you are running CentOS 5.1, FUSE support is configured upon installation. If you are running CentOS 5.5, FUSE support is built into the kernel. If you have upgraded from CentOS 5.1 to CentOS 5.5, you may not have FUSE support in your running kernel. If this is the case, please install the relevant FUSE packages before running the endpoint installer.

Virtualized environments

TRITON AP-ENDPOINT DLP can be installed on endpoint clients running Windows in Citrix XenDesktop Virtual Desktop Infrastructure (VDI) environments. The following operating systems are supported:

- Citrix XenDesktop 5.6
  - Windows XP
  - Windows 7
- Citrix XenDesktop 7.1
  - Windows Server 2008 R2
  - Windows XP
  - Windows 7

It can also be installed on the following VMWare platforms:

- VMware View Horizon VDI v5.2
  - Windows 7 (32- and 64-bit)
  - Windows Server 2008 (64-bit)

Browser support

TRITON AP-ENDPOINT Web

Except where indicated, the following web browsers fully support the TRITON AP-ENDPOINT Web client on both 32-bit and 64-bit operating systems:

Windows endpoints

- Internet Explorer up to v11
- Firefox up to v33
- Safari up to v5.x

- Google Chrome up to v38 (32-bit only)
- Opera up to v24

Mac endpoints

- Firefox up to v33
- Safari up to v8.x
- Google Chrome up to v38 (32-bit only)
- Opera up to v24

Full support means that the browser supports all installation methods, and both policy enforcement and proxy manipulation. In addition to enforcing browser traffic, TRITON AP-ENDPOINT Web also enforces other Internet-enabled applications.

TRITON AP-ENDPOINT DLP

When TRITON AP-ENDPOINT DLP analyzes data via the Web > Endpoint HTTP/HTTPS destination, it intercepts HTTP(S) posts as they are being uploaded within the browser. (It does not monitor download requests.)

The system analyzes posts from the following browsers:

Windows endpoints

- Internet Explorer up to v11
- Firefox up to v33
- Google Chrome 32-bit up to v38. (Endpoints using Chrome 33 or later must belong to a domain for the TRITON AP-ENDPOINT DLP Chrome extension to function.)

Mac endpoints

- Firefox to v33
- Google Chrome 32-bit up to v38
- Safari up to v7.1

The system does not support the HTTP destination channel on Linux endpoints.

DLP channel support

Email clients

TRITON AP-DATA analyzes all email messages sent from endpoint users, even if they send them to external Web mail services such as Yahoo.

For Windows, Websense TRITON AP-DATA can analyze endpoint email generated by Microsoft Outlook and IBM Lotus Notes. It supports the desktop version of Outlook 2003, 2007, 2010, and 2013 but not the Windows 8 touch version. If you are

using Outlook 2003, then Office 2003 SP3 must be installed. TRITON AP-DATA supports IBM Lotus Notes version 8.5.1, 8.5.2 FP4, and 8.5.3.

For Mac OS X, TRITON AP-DATA can analyze endpoint email generated by Outlook 2008, Outlook 2011, and Apple Mail.

Printer drivers

You can monitor data being sent from an endpoint machine to a local or network printer. TRITON AP-DATA supports drivers that print to a physical device, not those that print to file or PDF.

Application controls

You can monitor or prevent sensitive data from being copied and pasted from an application such as Microsoft Word or a Web browser. This is desirable, because endpoint clients are often disconnected from the corporate network and can pose a security risk.

TRITON AP-DATA can monitor copy and paste operations on most browsers, such as Internet Explorer, Firefox, Safari, and Opera.

It can also control access to files. For example, you can monitor uploads to cloud storage clients like DropBox and also IM / VOIP clients like GoToMeeting or Lync.

The applications that TRITON AP-DATA supports out of the box are found in the Technical Library article, TRITON AP-DATA Endpoint Applications. You can also add custom applications.

Supported removable media

- **Removable media** - You can monitor or prevent sensitive data from being transferred to removable media such as thumb drives and external hard drives. If desired, you can configure endpoint policies to encrypt files being transferred to removable media.
- **CD/DVD writers** - TRITON AP-DATA monitors unencrypted data being copied to native Windows and Mac CD/DVD burner applications. It monitors non-native Windows CD/DVD burner applications as well, but only blocks or permits operations without performing content classification.

  Non-native CD/DVD blocking applies to CD, DVD, and Blue-ray read-write devices on Windows 7, Windows 8, Windows Server 2008 R2, and Windows Server 2012 endpoints.

  Linux endpoint does not support CD/DVD burners.
- **Mobile devices** - On Windows 7, TRITON AP-DATA can also monitor unencrypted data being copied to Android devices through the Windows Portable Devices (WPD) protocol. This allows you to use application file access monitoring on software clients like Apple iTune and Samsung Kies when needed.

LAN control

Users commonly take their laptops home and then copy data through a LAN connection to a network drive or share on another computer. They also commonly take data from a shared folder (at work) to copy onto their laptop. With TRITON AP-DATA you can control LAN operations to protect your data.

Endpoint LAN control is applicable to Microsoft sharing only.

Destination channels by operating system

Not all destination channels apply to all operating systems. Endpoint destination support is shown below.

Destination Channel	Windows	Mac OS X	Linux
Email	✓	✓	
Web HTTP/HTTPS	✓	✓	
Printing	✓		
Applications	✓	* ✓	
Removable media	✓	✓	✓
LAN	✓	✓	

*Cloud apps and screen capture operations are not supported on Mac endpoints. The cut, copy, paste, file access, and download operations are not supported for cloud apps on Windows endpoints when they are used through a Windows Store browser.

Obtaining or Creating the Installation Package

Applies to:	In this topic
◆ TRITON AP-WEB v8.0.x ◆ TRITON AP-DATA v8.0.x ◆ Web Filter & Security v8.0.x ◆ TRITON AP-ENDPOINT Web v8.0.x ◆ TRITON AP-ENDPOINT DLP v8.0.x	◆ *Downloading installation packages from the TRITON Manager* ◆ *Creating installation packages from a package builder*

You can obtain endpoint installation packages in one of 2 ways:

- Download them from the TRITON Manager or Cloud TRITON Manager console (for hybrid or cloud web deployments that don't include DLP)
- Create them using the Websense TRITON AP-ENDPOINT Package Builder (for remote filter, DLP, hybrid, and mixed deployments)

Before beginning this process, you must install the TRITON APX product that is relevant to your environment: TRITON AP-WEB (Cloud or Hybrid module) or TRITON AP-DATA (DLP module). Refer to the Websense Technical Library for instructions.

Downloading installation packages from the TRITON Manager

If you are planning to deploy TRITON AP-ENDPOINT Web alone, you can download an endpoint installation package from your management console. If needed—for example, if you don't have Internet access—you can use the Websense TRITON AP-ENDPOINT Package Builder instead.

If you plan to use TRITON AP-ENDPOINT DLP or Remote Filtering Client, you must use the package builder.

On-premises TRITON Manager (hybrid deployments)

Customers with on-premises TRITON AP-WEB installations can log onto the Web module of the TRITON Manager and then navigate to **Settings > Hybrid Configuration > Hybrid User Identification** to obtain the endpoint installation package.

- You must set an anti-tampering password to enable the package download links.
- Different endpoint packages are available for 32-bit and 64-bit clients; select the appropriate package (or combination of packages) from the list provided.
- Use the GPO command that is provided if you intend to deploy the TRITON AP-ENDPOINT MSI package to client machines via GPO.

See the TRITON AP-WEB Administrator Help for more information about hybrid deployments of TRITON AP-ENDPOINT Web.

Cloud TRITON Manager (cloud deployments)

Customers with a full-cloud deployment (TRITON AP-WEB with the Web Cloud module) can log onto the Cloud TRITON Manager, and then navigate to **Web > Endpoint** to obtain the endpoint installation package.

- You must set an anti-tampering password to enable the package download links.
- Different endpoint packages are available for 32-bit and 64-bit clients; select the appropriate package (or combination of packages) from the list provided.
- Use the GPO command that is provided if you intend to deploy the TRITON AP-ENDPOINT MSI package to client machines via GPO.

See the Getting Started Guide for TRITON AP-WEB with Web Cloud Module for more information about cloud deployments of TRITON AP-ENDPOINT Web.

Creating installation packages from a package builder

If you are using TRITON AP-ENDPOINT DLP (alone or with TRITON AP-ENDPOINT Web) or you are using Remote Filter, you must use the Websense TRITON AP-ENDPOINT Package Builder to create a custom endpoint installation package.

If you are using TRITON AP-ENDPOINT Web alone, you can obtain the installation package from the TRITON Manager or Cloud TRITON Manager or use the package builder.

The installation package (a single executable file) is used to deploy the endpoint clients to user machines.

The endpoint package builder is a Windows utility that can be used to create 32- and 64-bit Windows packages, Mac packages, or (DLP only) Linux endpoint clients.

The utility can be found on any Windows server that includes TRITON AP-WEB, Web Filter & Security, or TRITON AP-DATA.

> **Note**
> The packages created by the Websense Endpoint Package Builder are backwards compatible with previous endpoint versions.

1. Launch the Websense TRITON AP-ENDPOINT Package Builder.

   For on-premises deployments, do one of the following on the TRITON management server:

   - **TRITON AP-WEB** or **Web Filter & Security -** Navigate to C:\Program Files (x86)\Websense\Web Security\DTFAgent\RemoteFilteringAgentPack\
   - **TRITON AP-DATA -** Select Start > All Programs > Websense > TRITON AP-DATA > Endpoint Package Builder
   - On Windows Server 2012, browse to the Start page and select **Endpoint Package Builder**.

   For cloud web deployments:

   - Log onto MyWebsense.com.
   - Navigate to TRITON AP-ENDPOINT, select a version, and then download the package builder.

   The Websense TRITON AP-ENDPOINT Package Builder utility extracts required files and launches.

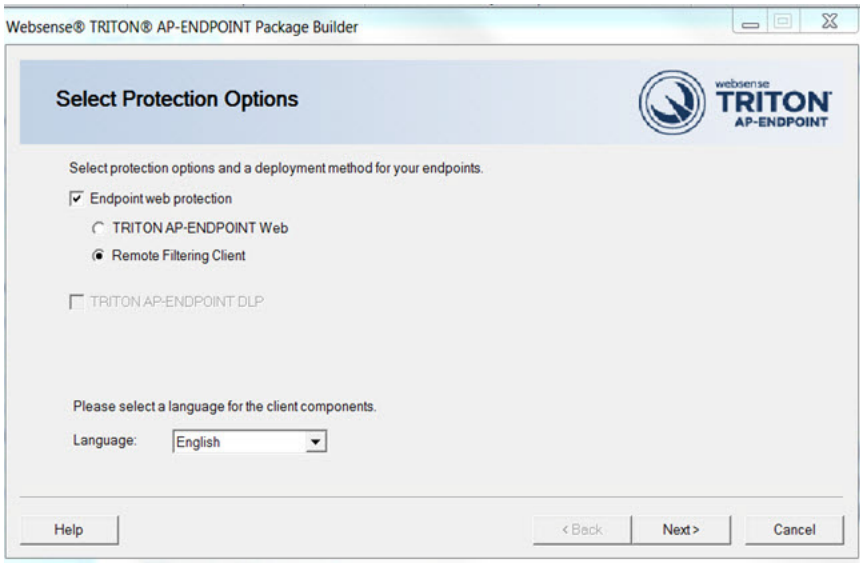
2. On the **Select Protection Options** screen, select one or both of the following:

   - **Endpoint web protection** provides web security to your endpoint devices.
   - **TRITON AP-ENDPOINT DLP** for data loss protection (requires TRITON AP-DATA)

   Under Endpoint web protection, select one of the following:

   - **TRITON AP-ENDPOINT Web** - choose this if you want to provide web protection in a full cloud deployment (requires TRITON AP-WEB with the Web Cloud module) or in a hybrid cloud/on-premises deployment (requires TRITON AP-WEB with the Web Hybrid module).

- **Remote Filtering Client** - choose this if you want to provide just remote filtering of endpoint clients (requires TRITON AP-WEB or Web Security & Filtering).

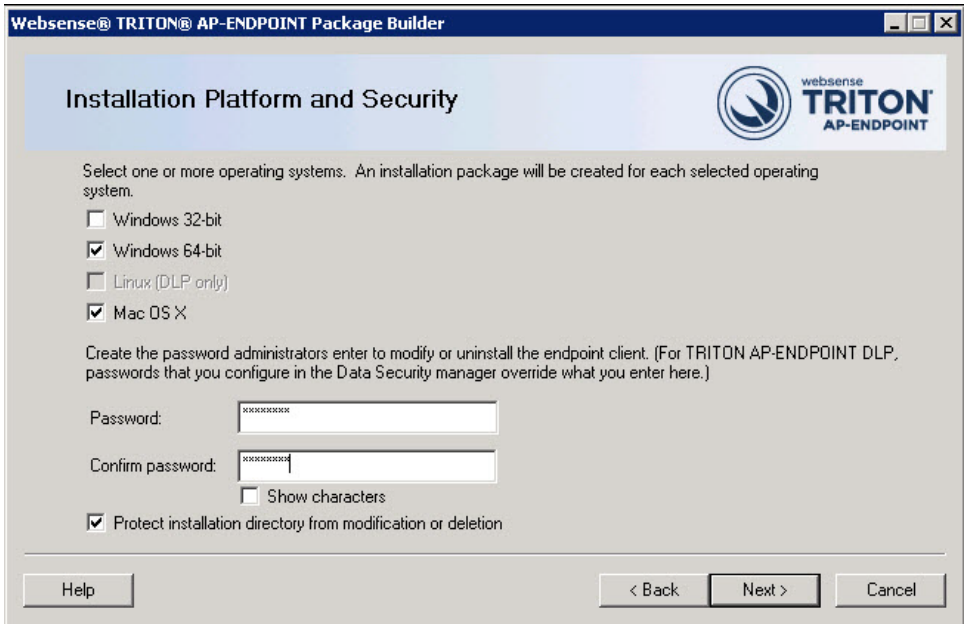


Also select a language for the client components.

In the TRITON Manager, you can change the language used for displaying messages to TRITON AP-ENDPOINT DLP users, but the language displayed in the user interface (buttons, captions, fields, etc.) can only be set during packaging.

Click **Next** when you're done.

3. On the **Installation Platform and Security** screen, select the operating system or systems for which you want to create an installation package, create the administrator password that will be used to uninstall or modify endpoint client software, and configure anti-tampering settings. When you are finished, click **Next**.


Websense® TRITON® AP-ENDPOINT Package Builder
Installation Platform and Security
websense
TRITON
AP-ENDPOINT
Select one or more operating systems. An installation package will be created for each selected operating system.
Windows 32-bit
Windows 64-bit
Linux (DLP only)
Mac OS X
Create the password administrators enter to modify or uninstall the endpoint client. (For TRITON AP-ENDPOINT DLP, passwords that you configure in the Data Security manager override what you enter here.)
Password:
Confirm password:
Show characters
Protect installation directory from modification or deletion
Help
< Back
Next >
Cancel

- You can create Windows (32-bit or 64-bit) or Mac OS X installation packages for endpoint web deployments or for deployments with both endpoint web and DLP features. If you are creating a stand-alone TRITON AP-ENDPOINT DLP package, you can also choose Linux.
- For security purposes, anyone who tries to modify or uninstall endpoint software is prompted for a password.

  Once the endpoint client contacts the server, this password is overwritten with the password specified by a TRITON administrator. Set this password in one of the following places (it is not necessary to do it in both):

  - TRITON AP-ENDPOINT DLP: In the Data module of TRITON Manager, go to **Settings > General > System > Endpoint**, then on the General tab, select **Enable endpoint administrator password**, and enter and confirm a password.
  - Endpoint web protection (Hybrid module): In the Web module of TRITON Manager, go to **Settings > Hybrid Configuration > Hybrid User Identification**, then enter and confirm an anti-tampering password.

    Endpoint web protection (Cloud module): In the Cloud TRITON Manager, go to **Web** > **Endpoint > Deployment Settings > Set Anti-Tampering Password**, and enter and confirm a password.

  Note that password hashes are stored in an encrypted file. The system does not store plain text passwords.

  If no password is specified, every user with admin privileges is able to uninstall the endpoint software from their computer.

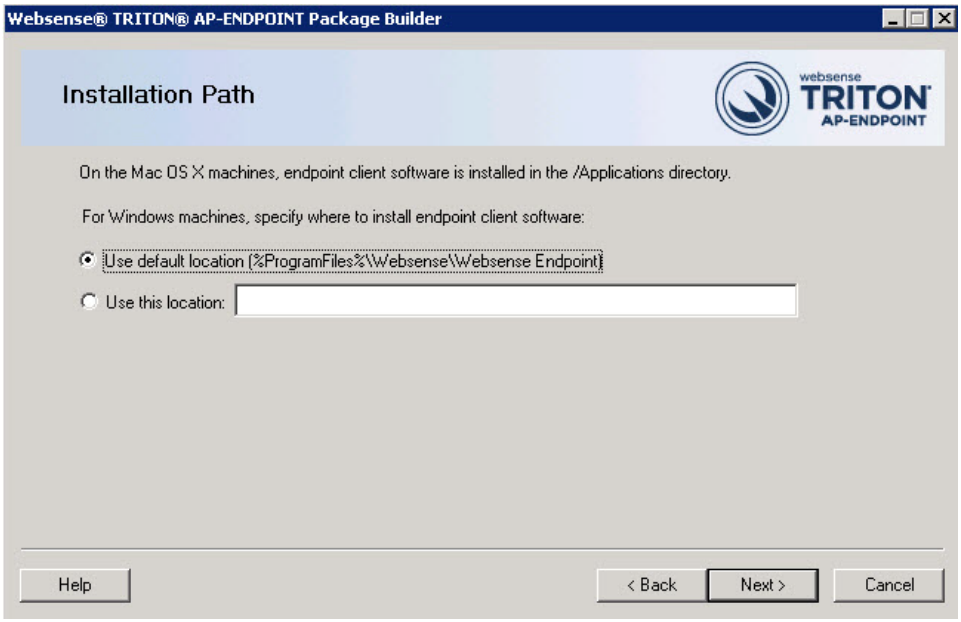
Click **Show characters** to display the password characters while you type.

- Sometimes when users cannot modify or uninstall the endpoint software, they try to delete the directory where the software is installed.

  Click **Protect installation directory from modification or deletion** if you do not want users to be able to perform these functions.

4. On the **Installation Path** screen, specify the directory to use for installing endpoint software on each endpoint device. The directory path must contain only English characters.

   Note that this screen does not appear if you are creating only a Mac OS X endpoint package. On Mac OS X machines, the endpoint client is installed in the /Applications directory.

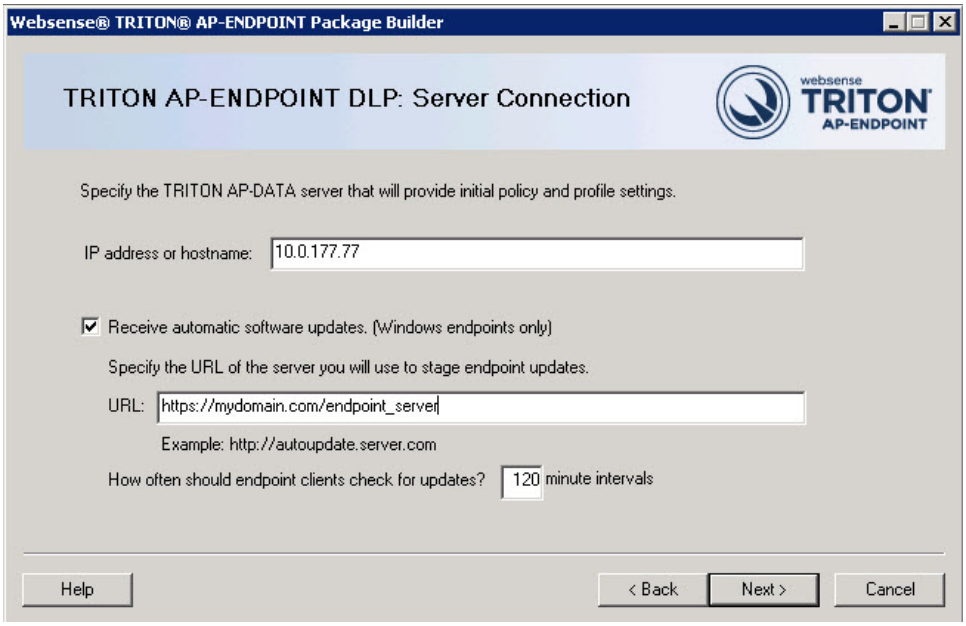

Websense® TRITON® AP-ENDPOINT Package Builder
Installation Path
websense
TRITON
AP-ENDPOINT
On the Mac OS X machines, endpoint client software is installed in the /Applications directory.
For Windows machines, specify where to install endpoint client software:
Use default location (%ProgramFiles%\Websense\Websense Endpoint)
Use this location:
Help
< Back
Next >
Cancel

   - **Use default location**: The endpoint software is installed in a default directory: \Program Files\Websense\Websense Endpoint (*Windows*) or /opt/websense/LinuxEndpoint (*Linux*).
   - **Use this location**: Manually specify the installation path for the endpoint software. Environment variables are supported.

5. Click **Next**.

TRITON AP-ENDPOINT DLP module

1. If you subscribe to the TRITON AP-ENDPOINT DLP module, the Server Connection screen appears:


Websense® TRITON® AP-ENDPOINT Package Builder
TRITON AP-ENDPOINT DLP: Server Connection
websense TRITON AP-ENDPOINT
Specify the TRITON AP-DATA server that will provide initial policy and profile settings.
IP address or hostname:
10.0.177.77
Receive automatic software updates. (Windows endpoints only)
Specify the URL of the server you will use to stage endpoint updates.
URL:
https://mydomain.com/endpoint_server
Example: http://autoupdate.server.com
How often should endpoint clients check for updates?
120
minute intervals
Help
< Back
Next >
Cancel

IP address or hostname: Provide the IP address or hostname of the TRITON AP-DATA server that endpoint machines should use to retrieve initial profile and policy information. (Once configured, endpoints retrieve policy and profile updates from the endpoint server defined in their profiles.)

Receive automatic software updates (Windows endpoints only): When new versions of the endpoint are released, you may upgrade the software on each endpoint—this can be done via GPO or SMS—or you can configure automatic updates on this screen.

You cannot use the auto-update feature in the Web module of the TRITON Manager to automate updates for combined web and DLP endpoints.

This option does not apply to Linux or Mac endpoints.

To automate software updates for DLP or combined web/DLP endpoints:

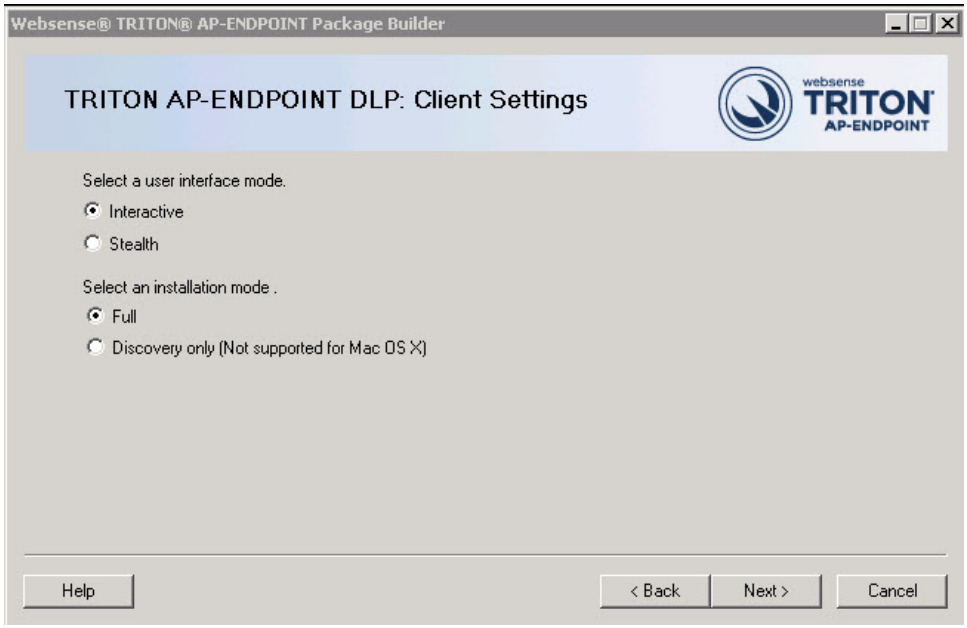
a. Prepare a server with the latest updates on it (see "Configuring the auto-update server" for details).

b. Select **Receive automatic software updates**.

c. Specify the URL of the server you created. (It cannot be secure http (https).)

d. Indicate how often you want endpoint machines to check for updates.

2. Click **Next** and the Client Settings screen appears:



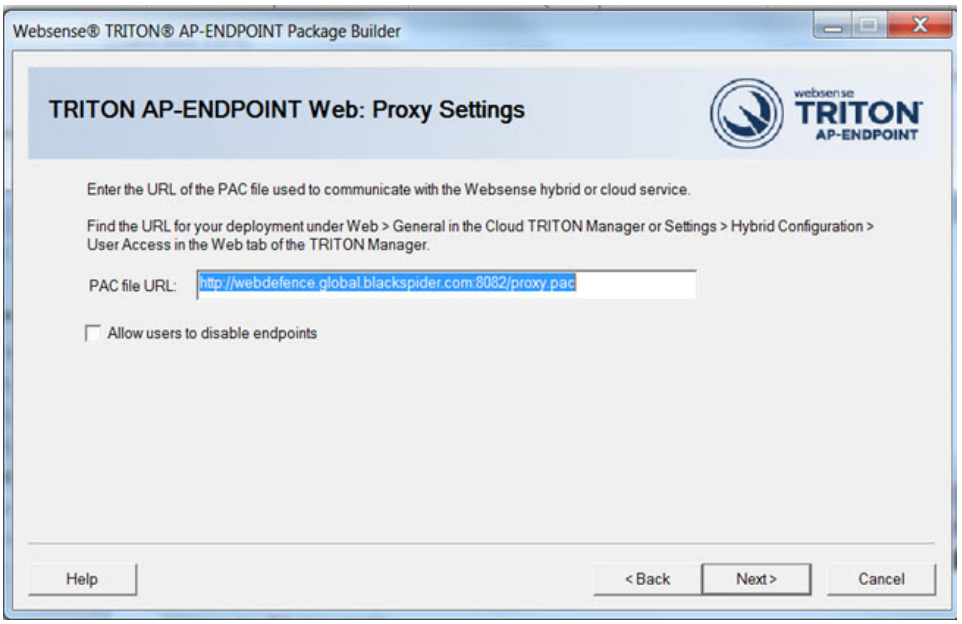
Complete the fields as follows:

User interface mode	Select from the following 2 options: • **Interactive**: A user interface is displayed on all endpoint machines. Users know when files have been contained and have the option to save them to an authorized location. • **Stealth**: The TRITON AP-ENDPOINT DLP user interface is not displayed to the user. Because they don't see block notifications or continuation dialogs, this mode is best reserved for discovery tasks and audit-only policies. Note that you must reinstall the endpoint and deploy a new profile to switch user interface modes.
Installation Mode	Applies to Windows only. Select from the following 2 options: • **Full**: Installs the endpoint with full policy monitoring and blocking capabilities upon a policy breach. All incidents are reported in the TRITON Manager. Endpoints that are installed in Full Mode require a reboot. • **Discovery Only**: Configures the endpoint to run discovery analysis but not DLP. Discovery Only installation does not require a reboot.

3. Click **Next**.

TRITON AP-ENDPOINT Web

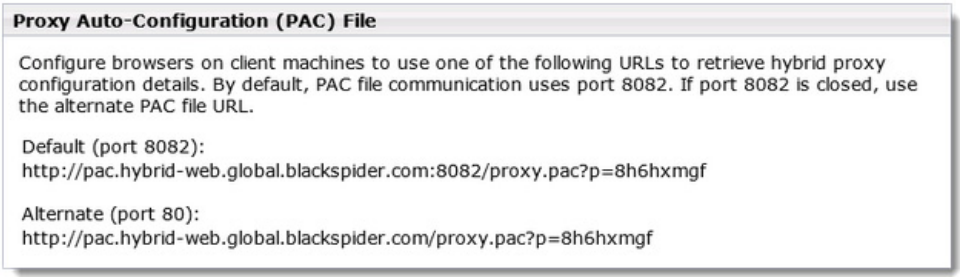
1. Use the **Proxy Settings** screen to specify the URL for your organization's PAC file.


Websense® TRITON® AP-ENDPOINT Package Builder
TRITON AP-ENDPOINT Web: Proxy Settings
websense
TRITON
AP-ENDPOINT
Enter the URL of the PAC file used to communicate with the Websense hybrid or cloud service.
Find the URL for your deployment under Web > General in the Cloud TRITON Manager or Settings > Hybrid Configuration > User Access in the Web tab of the TRITON Manager.
PAC file URL:
http://webdefence.global.blackspider.com:8082/proxy.pac
Allow users to disable endpoints
Help
< Back
Next >
Cancel

Replace the default URL with the customized URL for your deployment.

Hybrid deployments

For *hybrid* deployments, the URL can be found on the **Settings > Hybrid Configuration > User Access** page in the Web module of the TRITON Manager.


Proxy Auto-Configuration (PAC) File
Configure browsers on client machines to use one of the following URLs to retrieve hybrid proxy configuration details. By default, PAC file communication uses port 8082. If port 8082 is closed, use the alternate PAC file URL.
Default (port 8082):
http://pac.hybrid-web.global.blackspider.com:8082/proxy.pac?p=8h6hxmgf
Alternate (port 80):
http://pac.hybrid-web.global.blackspider.com/proxy.pac?p=8h6hxmgf

Select the URL appropriate for your environment (either port 8082 or port 80). For example:

```
Default (port 8082): http://pac.hybrid-
web.global.blackspider.com:8082/proxy.pac?p=8h6hxmgf
```

```
Alternate (port 80): http://pac.hybrid-
web.global.blackspider.com/proxy.pac?p=8h6hxmgf
```

In this example, **8h6hxmgf** is a unique identifier for an organization. Yours will be different. Yours explicitly defines *your* organization.

Note the difference between the sub-domains of the default PAC file URL and the sample customized URL. The “hybrid-web” sub-domain is used for on-premises TRITON AP-WEB deployments that use TRITON AP-ENDPOINT.

Full cloud deployments

For *full cloud* deployments, the “webdefence” sub-domain is used. For example, a policy-specific PAC file URL looks something like this:

```
Default (port 8082): http://
webdefence.global.blackspider.com:8082/
proxy.pac?p=8h6hxmgf
```

```
Alternate (port 80): http://
webdefence.global.blackspider.com/proxy.pac?p=8h6hxmgf
```

In this example, **8h6hxmgf** is a unique identifier for an organization. Yours will be different. Yours explicitly defines *your* organization.

You can find policy-specific URLs for your cloud deployment on the General tab of a policy in the Cloud TRITON Manager. If you would rather use an account-level PAC file, navigate to the **Web > General** page to find the PAC file URL.

Allow users to disable endpoints

Select **Allow users to disable endpoints (Windows endpoints only)** if you want to allow users to disable the web protection on their on client machines, for example if you want them to edit local proxy settings. Be aware that selecting this option allows users to circumvent the protections offered by the endpoint software.

Click **Next**.

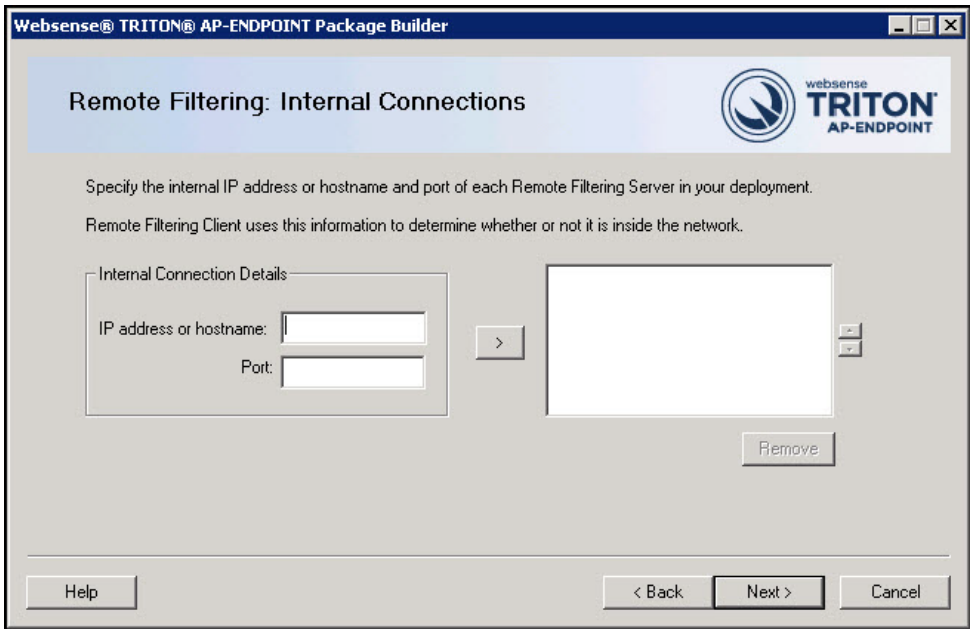
Remote filter

1. Prepare Remote Filtering Server components as described here.
2. On the **Internal Connections** screen, enter the internal IP address or hostname and internal Port of each Remote Filtering Server to which this client will connect. Use the **>** button to move the information to the selected list. When you are finished, click **Next**.

   Remote Filtering Client sends its heartbeat to these IP addresses and ports to determine whether or not it is inside the network.

   If you have multiple Remote Filtering Server instances, Remote Filtering Client rotates through the list in order until a functioning server is located.

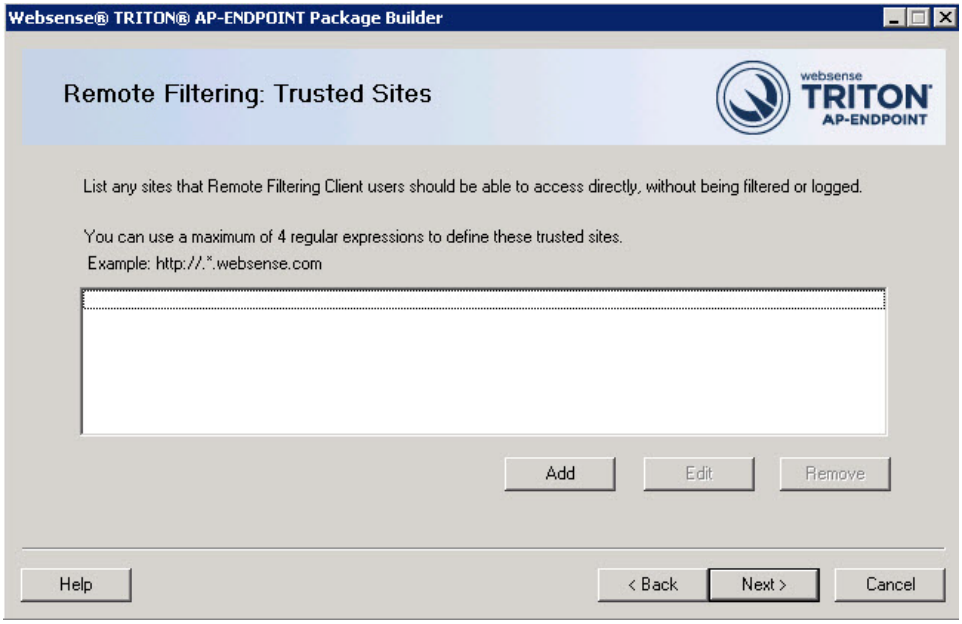
   Remote Filtering Server has a 2-minute inactivity timeout period. If the client connects, and then does not send an Internet request in the timeout period, the server drops the connection. When the next request is made, Remote Filtering Client goes through its list to connect again. This protects server performance by reducing the number of unused connections that might otherwise accumulate.

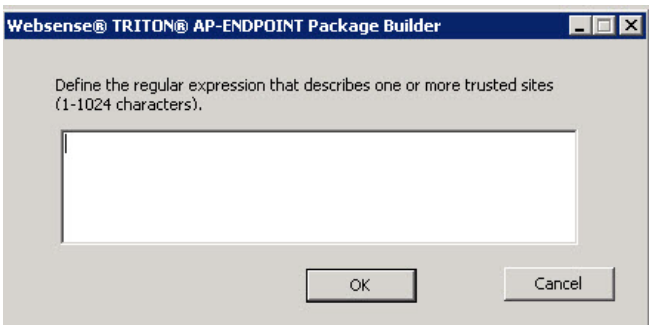

Websense® TRITON® AP-ENDPOINT Package Builder
Remote Filtering: Internal Connections
websense
TRITON
AP-ENDPOINT
Specify the internal IP address or hostname and port of each Remote Filtering Server in your deployment.
Remote Filtering Client uses this information to determine whether or not it is inside the network.
Internal Connection Details
IP address or hostname:
Port:
>
Remove
Help
< Back
Next >
Cancel

Indicate whether or not to **Log user Internet activity** seen by Remote Filtering Client instances installed using this customized installation package, and then click **Next**.

3. Use the **Trusted Sites** list to enter up to 4 URLs, IP addresses, or regular expressions for sites that Remote Filtering Client users can access directly, without being filtered or logged. Click **Add** to enter a URL, IP address, or regular expression.

When you are finished, click **Next**.

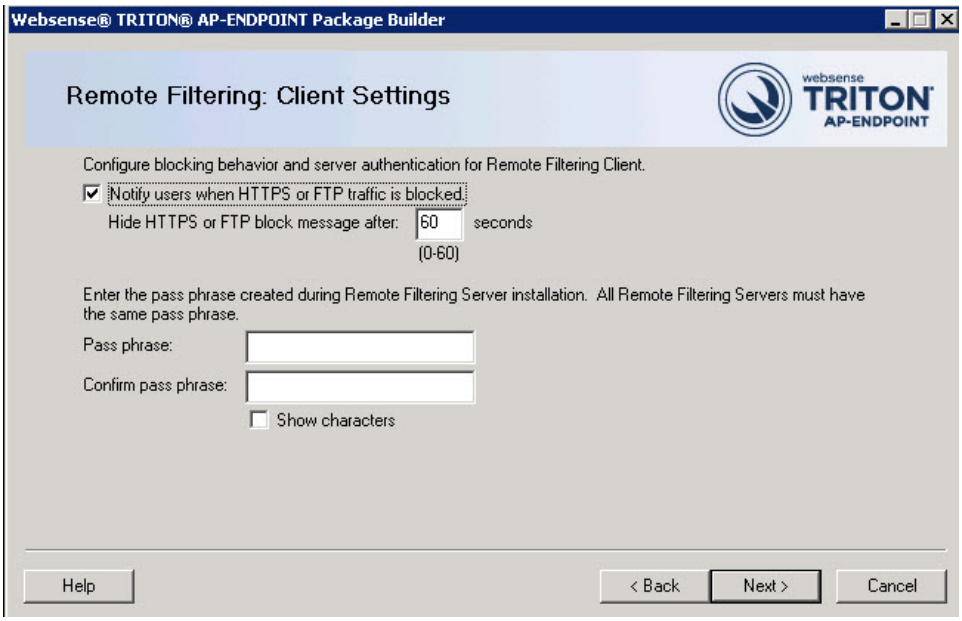

Websense® TRITON® AP-ENDPOINT Package Builder
Remote Filtering: Trusted Sites
websense
TRITON
AP-ENDPOINT
List any sites that Remote Filtering Client users should be able to access directly, without being filtered or logged.
You can use a maximum of 4 regular expressions to define these trusted sites.
Example: http://.*.websense.com
Add
Edit
Remove
Help
< Back
Next >
Cancel


Websense® TRITON® AP-ENDPOINT Package Builder
Define the regular expression that describes one or more trusted sites (1-1024 characters).
OK
Cancel

4. Indicate whether or not to **Notify users when HTTPS or FTP traffic is blocked**, then, if notification is enabled, specify how long (in seconds) the message is displayed.

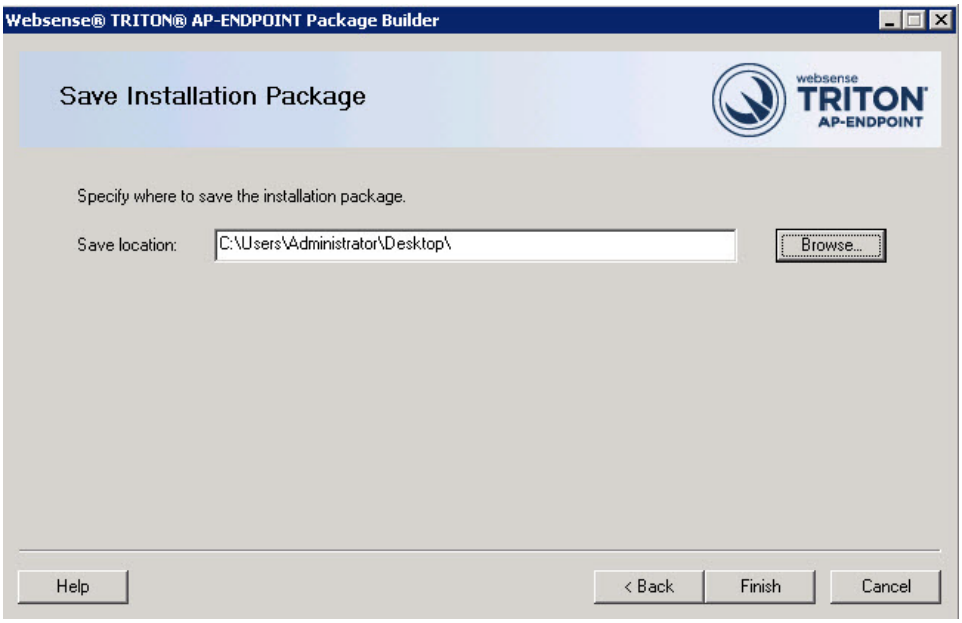
   Enter and confirm the **Pass phrase** used for communication with Remote Filtering Server. This must match the pass phrase created when Remote Filtering Server was installed.

When you are finished, click **Next**.


Websense® TRITON® AP-ENDPOINT Package Builder
Remote Filtering: Client Settings
websense TRITON AP-ENDPOINT
Configure blocking behavior and server authentication for Remote Filtering Client.
Notify users when HTTPS or FTP traffic is blocked
Hide HTTPS or FTP block message after: 60 seconds
(0-60)
Enter the pass phrase created during Remote Filtering Server installation. All Remote Filtering Servers must have the same pass phrase.
Pass phrase:
Confirm pass phrase:
Show characters
Help
< Back
Next >
Cancel

Global settings

1. When you're done configuring your endpoint selections, use the **Save Installation Package** screen to enter a directory path to use for storing the installation package before it is deployed to client machines.



   Either manually enter a path or click **Browse** to find the location.
2. Click **Finish**.

You'll see a system message if the package is created successfully. If the creation of the package fails, you'll see an error message. If this happens, contact Websense Technical Support for assistance.

3. Click **OK**.

   Once the packaging tool has finished, the packages are created in the designated path. Refer to *Deploying endpoint software in Your Enterprise*, page 21 for instructions on distributing the package to the endpoint devices.

Deploying endpoint software in Your Enterprise

Applies to:	In this topic
◆ TRITON AP-WEB v8.0.x ◆ TRITON AP-DATA v8.0.x ◆ Web Filter & Security v8.0.x ◆ TRITON AP-ENDPOINT Web v8.0.x ◆ TRITON AP-ENDPOINT DLP v8.0.x	◆ *Before you begin* ◆ *Deploying Windows endpoints* ◆ *Deploying Mac endpoints* ◆ *Deploying Linux endpoints (stand-alone DLP only)* ◆ *Configuring and managing endpoints* ◆ *Uninstalling endpoint software*

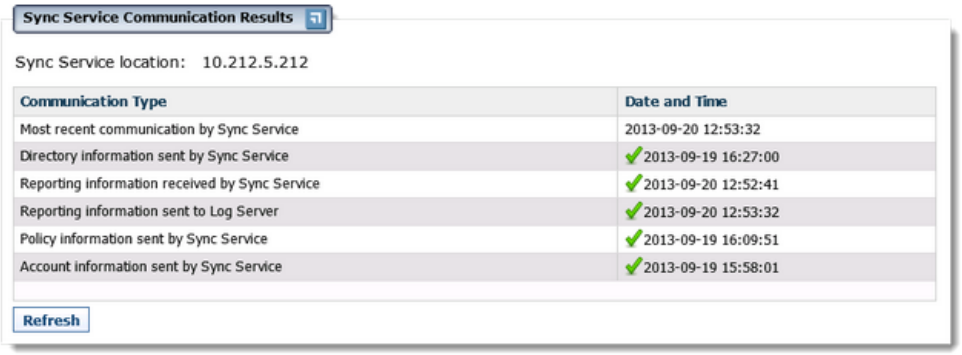
This section describes how to deploy DLP and mixed endpoint installation packages. For information on deploying TRITON AP-ENDPOINT Web only packages, see *On-premises TRITON Manager (hybrid deployments)*, page 10 or *Cloud TRITON Manager (cloud deployments)*, page 10.

Before you begin

- For best practice, start by deploying and testing endpoint software to a few local network machines, then increase to a limited number of remote machines before deploying the software throughout your enterprise.
- Check that your endpoint machines meet the minimum system requirements. See *System requirements*, page 3 for details.
- Exclude the following directories from any antivirus software that is deployed to endpoint clients:
  - The endpoint installation folder
  - Endpoint processes:
    - **wepsvc.exe**
    - **dserui.exe**
    - **ProxyUI.exe**
    - **RFUI.exe**

- **EndpointClassifier.exe** and **kvoop.exe**

- Ensure the endpoint installation path is not being encrypted by disk encryption software.
- If you are including DLP, ensure that the auto-update feature in the Web module of the TRITON Manager is disabled. If you want auto-updates, you can use the TRITON AP-DATA method described below. (Windows only)
- For hybrid web deployments, make sure that your user accounts are synchronized with the hybrid service. To verify, log into the Web module of the TRITON Manager and select **Main > Status > Hybrid Service**. It is okay if you have not yet used the hybrid service.



Disabling automatic updates for TRITON AP-ENDPOINT Web

1. Go to the **Settings > Hybrid Configuration > Hybrid User Identification** page in the Web module of TRITON Manager.
2. Deselect **Enable installation and update of Web Endpoint on client machines**.
3. Deselect **Automatically update endpoint installations when a new version is released**.
4. Click **OK** to cache your changes. Changes are not implemented until you click **Save All**.

> **Note**
> At the completion of any endpoint update, you must restart the endpoint for the updates to take effect.

Enabling automatic updates

Windows only. To deploy endpoint updates automatically, you must create an update server that hosts endpoint installation packages. See "Automatic Updates for Websense data endpoints" for details.

You must also select **Receive automatic updates for data endpoints** on the Websense TRITON AP-ENDPOINT Package Builder "Server Connections" screen. On this same screen, specify the URL of the server you created and indicate how often you want endpoint machines to check for updates (every 2 hours by default).

When configured properly, your update server pushes software updates out to endpoint machines and installs the packages in the background silently.

> **Note**
> If you want to change the components installed on an endpoint client with components of the same version (for example, switch from a mixed deployment to a stand-alone DLP deployment), you must use the package builder to generate a new package and use one of the other deployment options to deploy it. You cannot use the auto-update feature to update endpoints with the same version.

Deploying Windows endpoints

> **Important**
> After deploying the installation package, you must restart the endpoint software to complete the installation process.

There are a few ways to distribute the endpoint software on Windows clients, including virtual desktop clients running Windows:

- Manually on each endpoint device

  See *Manual deployment*, page 23.
- Using System Center Configuration Manager (SCCM) or Systems Management Server (SMS)

  See Creating and distributing Websense endpoints using SCCM or SMS for details.
- Using a Microsoft Group Policy Object (GPO) or other third-party deployment tool for Windows. If you need assistance, contact Websense Technical Support.

Manual deployment

Windows packages contain a single executable file: **WebsenseTRITONAP-ENDPOINT-x32.exe** or **WebsenseTRITONAP-ENDPOINT-x64.exe**.

Copy one of these self-extracting executable files to the client machine.

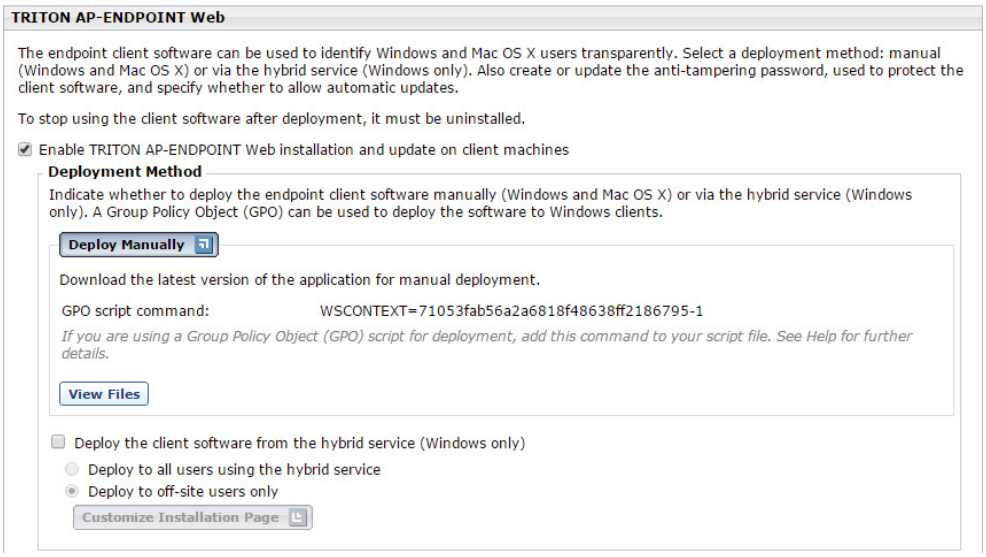
For stand-alone TRITON AP-ENDPOINT DLP installations, double-click the executable file and step through the installation wizard.

For web, cloud, or mixed deployments, run the following command instead of double-clicking the installer:

```
WebsenseTRITONAP-ENDPOINT-x64.exe /v"XPSWD=<password>
WSCONTEXT=<token>"
```

where:

- <password> is the anti-tampering password used by the previous-version endpoint client (if upgrading) or to be used by the new endpoint.
- <token> is the WSCONTEXT value displayed in the GPO command string on the **Settings > Hybrid Configuration > Hybrid User Identification** page in the Web module of the TRITON Manager or the **Web > Endpoint** page in the Cloud TRITON Manager. For example:


TRITON AP-ENDPOINT Web
The endpoint client software can be used to identify Windows and Mac OS X users transparently. Select a deployment method: manual (Windows and Mac OS X) or via the hybrid service (Windows only). Also create or update the anti-tampering password, used to protect the client software, and specify whether to allow automatic updates.
To stop using the client software after deployment, it must be uninstalled.
Enable TRITON AP-ENDPOINT Web installation and update on client machines
Deployment Method
Indicate whether to deploy the endpoint client software manually (Windows and Mac OS X) or via the hybrid service (Windows only). A Group Policy Object (GPO) can be used to deploy the software to Windows clients.
Deploy Manually
Download the latest version of the application for manual deployment.
GPO script command:
WSCONTEXT=71053fab56a2a6818f48638ff2186795-1
If you are using a Group Policy Object (GPO) script for deployment, add this command to your script file. See Help for further details.
View Files
Deploy the client software from the hybrid service (Windows only)
Deploy to all users using the hybrid service
Deploy to off-site users only
Customize Installation Page

  The WSCONTEXT argument used to identify your organization to the hybrid or cloud service must be included in the command string. Each account has its own WSCONTEXT string. Roaming and remote users use this string to connect to your specific account.
- All arguments passed via the **/v** parameter must be enclosed in straight quotes, as shown in the example.

You must provide both the XPSWD and WSCONTEXT arguments.

To perform a silent install, add the /qn" parameter as follows:

```
WebsenseTRITONAP-ENDPOINT-x64.exe /v"/qn XPSWD=<password>
WSCONTEXT=<token>"
```

The MSI command switches are summarized below:

Function	MSI Switch
Silent install	WebsenseTRITONAP-ENDPOINT-x64.exe /v"/qn"
Set WSCONTEXT	WebsenseTRITONAP-ENDPOINT-x64.exe /v"WSCONTEXT=xxxx"
Set uninstall password	WebsenseTRITONAP-ENDPOINT-x64.exe /v"XPSWD=xxxx"
Set WSCONTEXT and silent install	WebsenseTRITONAP-ENDPOINT-x64.exe /v"/qn WSCONTEXT=xxxx"

In virtual desktop (VDI) environments, install the endpoint software as if the client machine were a physical machine, while taking into consideration any additional steps required by the infrastructure for third-party installations.

Testing deployment

To confirm that the endpoint software is installed and running on a machine:

- For endpoint web deployments, go to **Start > Administrative Tools > Services**. Check that **Websense SaaS Service** is present in the Services list and is started.
- When TRITON AP-ENDPOINT DLP is installed in interactive mode, an icon ( ) appears on the endpoint machine's task bar. Click the icon for status information. (No icon shows in stealth mode.)

Most failed endpoint installation issues are permission related. An endpoint installation requires local administrator rights.

Deploying Mac endpoints

There are a few ways to distribute the endpoint software:

- Manually on each endpoint device

  See *Manual deployment*, page 25.
- Using Remote Desktop (Mac OS X only)

  See Installing Mac endpoints with Remote Desktop for details.

Manual deployment

Mac packages contain a zip file, WebsenseTRITONAP-ENDPOINT_Mac.zip.

Copy WebsenseTRITONAP-ENDPOINT_Mac.zip to the client machine, and double-click the file.

1. Mac OS X automatically creates a directory named "EndpointInstaller," which contains a file called **WebsenseEndpoint.pkg**.
2. Double-click **WebsenseEndpoint.pkg** to start the installation process.
3. Click **Continue**, and agree to the license agreement.
4. Click **Install**.
5. Enter a user name and password for a user with administrator rights to install the software.

   You'll receive a confirmation message if the endpoint was successfully installed.

Testing deployment

To confirm that the endpoint is installed and running on a machine:

- Endpoint files are installed in the /Library/Application Support/Websense Endpoint/ directory.
- When TRITON AP-ENDPOINT DLP is installed and running in interactive mode, an icon ( ) appears on the endpoint machine's task bar. Click the icon for status information. (No icon shows in stealth mode.)

To check whether the endpoint is running, open 'Activity Monitor' and select 'All Processes' under the menu option 'View'. The process 'wspxyd', 'wsdlpd' or 'wsrfd' should be running depending on the endpoint product is installed.

Deploying Linux endpoints (stand-alone DLP only)

Linux packages contain the following installer: **LinuxEndpoint_SFX_installer_el5**. Use this installer with Red Hat Enterprise Linux version 5.x.

To install TRITON AP-ENDPOINT DLP software on a Linux computer, copy the installer to the machine and run it in the terminal console. Reboot the machine when done.

Configuring and managing endpoints

Once the endpoint software is deployed, endpoint web protection is automatically started. The policies and exceptions you created for users whose requests are managed by the hybrid service are applied automatically.

TRITON AP-ENDPOINT DLP requires configuration in the TRITON Manager. This entails:

1. Adding an endpoint profile to the Data module of the TRITON Manager or using the default. A default profile is automatically installed with the client package. (**Settings > Deployment > Endpoint**.)
2. Rearranging endpoint profiles. (**Settings > Deployment > Endpoint**.)
3. Configuring endpoint settings. (**Settings > General > System > Endpoint**.)
4. Creating endpoint resources. (**Main > Policy Management > Resources > Endpoint Devices/Endpoint Applications/Application Groups.**
5. Creating or modifying a rule for endpoint channels. (**Main > Policy Management > DLP / Discovery Policies**, Destination tab.)
6. Defining the type of endpoint machines to analyze, as well as the network location. (**Main > Policy Management > DLP / Discovery Policies**, Custom Policy wizard, Source tab.) Use the Network Location field to define the behavior of the endpoint on and off the network.

See the Data Security Manager Help for specific instructions.

To configure remote filtering settings, use the **Settings > General > Remote Filtering** page in the Web module of TRITON Manager. Refer to Web Administrator Help for details.

Uninstalling endpoint software

Windows uninstallation

You can uninstall endpoint software 2 ways:

- Locally on each endpoint client
- Remotely through a deployment server or distribution system

> **Note**
> If you configured an administrative password, you must supply it to uninstall the software.

Local uninstallation

1. Go to **Start > Control Panel > Add/Remove Programs**.
2. The Add/Remove Programs screen is displayed.
3. Scroll down the list of installed programs, select **TRITON AP-ENDPOINT** and click **Remove**.
4. Click **Yes** in the confirmation message asking if you are sure you want to delete the endpoint software.
5. You may be prompted to provide an administrative password, if you defined one. If so, enter the password in the field provided and click **OK**.
6. You'll see a system message indicating you must restart your system. Click **Yes** to restart or **No** to restart your system later. Once the computer has been restarted, the configuration changes apply.

Remote uninstallation with deployment server

If you use a deployment server to deploy endpoint software, you can perform a silent uninstall by running the following command (does not apply to stand-alone DLP).

```
msiexec /x {product_code} XPSWD=password /qn
```

where:

- `{product_code}` is a unique identifier (GUID) that can be found in the **setup.ini** file of each installation package or the system registry. It is different for each version and bit type (32- versus 64-bit).
- `password` is the administrator password that you entered when creating the installation package.

To find the **setup.ini** file, use a file compression tool like WinZip or 7-Zip to extract the contents of the installation package executable

To perform a silent uninstall that doesn't require a reboot, add the /norestart parameter as follows:

```
misexec /x{ProductCode}  /qn /XPSWD=xxxx /norestart
```

The MSI command switches are summarized below

Function	MSI Switch
Silent uninstall*	misexec /x{ProductCode} XPSWD=xxxx /qn
Silent uninstall without reboot*	misexec /x{ProductCode} XPSWD=xxxx /norestart /qn

Remote uninstallation using distribution systems

You can uninstall endpoint software remotely by using distribution systems. If you used an SMS distribution system to create packages for installation, those packages can be reused, with a slight modification, for uninstalling the software. If a package was not created for deployment of the endpoint software, a new one needs to be created for uninstalling.

To uninstall with package:

1. Follow the procedure for Creating and distributing Websense endpoints using SDCCM or SMS.
2. In step 1, select **Per-system uninstall**.
3. Complete the remaining procedures.
4. After deploying the package, Websense endpoint software will be uninstalled from the defined list of computers.

Mac uninstallation

1. Go to **System Preferences.**
2. In the **Other** section, click the icon for the Websense endpoint software.
3. Click **Uninstall Endpoint**.
4. Enter the local administrator name and password.
5. Click **OK**.
6. If you created an anti-tampering password to block attempts to uninstall or modify endpoint client software, enter that password.
7. Click **OK** to begin uninstalling the endpoint.
8. You'll receive a confirmation message if the endpoint was successfully uninstalled.

To uninstall the Mac endpoint remotely, you can use the following command line option with Apple Remote Desktop:

```
/usr/sbin/wepsvc --uninstall [--password pwd]
```

Linux uninstallation (stand-alone DLP only)

Run the **ep-uninstall** script (located by default at /opt/websense/LinuxEndpoint/ep-uninstall). You may be prompted for an administrative password, if one was defined by your system administrator.